REMARKS

The Office Action dated November 30, 2007, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

By this response, claims have been amended to more particularly point out and distinctly claim the subject matter of the present invention. Claims 14-20 have been added. No new matter has been added and no new issues are raised which require further consideration and/or search. Support for the above amendments are provided in the Specification in at least paragraphs [0028]-[0036]. Accordingly, claims 1-20 are currently pending in the application, of which claims 1, 10, 13-14, 16 and 18 are independent claims.

In view of the above amendments and the following remarks, Applicants respectfully request reconsideration and timely withdrawal of the pending claim rejections for the reasons discussed below.

Claim Rejections under 35 U.S.C. §102(e)

The Office Action rejected claims 1-6, 8, and 10-13 under 35 U.S.C. §102(e) as being allegedly anticipated by Ludovici, *et al.* (U.S. Patent No. 6,636,898) ("Ludovici"). Applicants respectfully submit that the claims recite subject matter that is neither disclosed nor suggested in Ludovici.

Claim 1, upon which claims 2-9 are dependent, recites a system. The system includes an application device, a service device, and a communication network configured to connect the application device to the service device. The system also includes an internet protocol security service configured to provide one or more internet protocol security services including at least one of authentication services and encryption services, at least one management client configured to issue security association management requests to create and manage, with a session key management protocol, security associations for use by the provided internet protocol security services, and a management server configured to receive the security association management requests issued from the at least one management client and to respond in connection with the internet protocol security service, to the security association management requests received at the management server. The internet protocol security service is deployed in the service device. The at least one management client is deployed in the application device. The management server is deployed in the service device.

Claim 10, upon which claims 11 and 12 are dependent, recites a method of remotely and transparently managing security associations of internet protocol security. The method includes providing one or more internet protocol security service including at least one of authentication services and encryption services from an internet protocol security service, issuing security association management requests to create and manage, with a session key management protocol, security associations for use by the provided internet protocol security services, from at least one management client, receiving in a

management server the security association management requests issued from the at least one management client, and responding, in connection with an internet protocol security service, to the security association management requests received at the management server. The internet protocol security service is deployed in a service device. The at least one management client is deployed in an application device. The management server is deployed in the service device. The application device is connected to the service device by a communication network.

Claim 13 recites a system. The system includes application means, servicing means, and communication means for connecting the application means with the servicing means. The system also includes internet protocol security service means for providing one or more internet protocol security services including at least one of authentication services and encryption services. The internet protocol security service means is deployed in the servicing means. The system further includes at least one management client means for issuing security association management requests to create and manage, with a session key management protocol, security associations for use by the provided internet protocol security services. The at least one management client means is deployed in the application means. The system further includes management server means for receiving the security association management requests issued from the at least one management client means and for responding, in connection with the internet protocol security service, to the security

association management requests received at the management server. The management server means is deployed in the servicing means.

As will be discussed below, Ludovici fails to disclose or suggest every claim feature recited in claims 1-6, 8, and 10-13, and therefore fails to provide the features of the claims discussed above.

Ludovici is directed to a central management of connections in a virtual private network implementing IPSec and ISAKMP protocols. To allow this, a VPN connection manager is provided that is operable to start, stop, delete and query instantiated VPN connections (Ludovici, Abstract; col. 2, lines 33-37). Ludovici primarily discusses the functionality of the VPN connection manager (VPNCNM) and various objects of which are depicted in Figure 1. Further, Figure 22 depicts an IKE Server 451, an IPSEC 452, and a VPNCNM 450 component. The VPNCNM 450 component requests security associations from the IKE Server 451. The IKE Server 451 negotiates an SA, and then responds to the VPNCNM 450 component. Then, the VPNCNM 450 transfers information to IPSEC 452 (Ludovici, Abstract; col. 8, line 47, to col. 9, line 21).

Applicants respectfully submit that Ludovici fails to disclose or suggest every feature recited in claim 1, and similarly recited in claims 10 and 13. Specifically, Ludovici fails to disclose or suggest at least three separate elements recited in claim 1, and similarly recited in claims 10 and 13.

an internet protocol security service configured to provide one or more internet protocol security services comprising at least one of authentication services and encryption services, said internet protocol security service deployed in said service device;

at least one management client configured to issue security association management requests to create and manage, with a session key management protocol, security associations for use by said provided internet protocol security services, said at least one management client deployed in said application device; and

a management server configured to receive said security association management requests issued from said at least one management client and to respond in connection with said internet protocol security service, to said security association management requests received at said management server, said management server deployed in said service device (emphasis added).

Referring to Figure 22, the Office Action alleged that Ludovici discloses the aforementioned features of claims 1, 10, and 13. The Office Action indicated that "one of ordinary skill in the art would reasonably ascertain that the IPSEC and IKE server may be separate, as their communication goes through a separate server" (See Office Action, *Response to Arguments*, on page 4). Further, the Office Action indicated that "since the correspondence between the VPNCNM and the IKE Server are networked requests, the IPSEC and IKE Server (as depicted in figure 22) must also be only communicatively connected, since they transact via the VPNCNM" (See Office Action on page 3). However, a review of Figure 22 and the disclosure of Ludovici demonstrates that Ludovici does not disclose the

aforementioned features recited in claim 1, and similarly recited in claims 10 and 13.

For example, Ludovici discloses IKE server 451, corresponding to a common prior art security association or key management application, and IPSEC 452, corresponding to a common prior art IPsec service means. Ludovici fails to explicitly state whether IKE server 451 and IPSEC 452 are deployed on a single device or in separate devices. One of ordinary skill in the art at the time the invention was made would have understood that IKE server 451 and IPSEC 452 in Ludovici were deployed in a single device, since this is the only implementation orientation known, as shown in Ludovici at col. 3, lines 23-25, with reference to co-pending U.S. Application No. 09/239,693, now U.S. Patent No. 6,330,562, issued to Boden, *et al.* ("Boden"), which Ludovici indicates contains related subject matter. Boden discloses that IKE application 16 and IPSec 202 for a one connection end-point are deployed on a single VPN node 18, i.e. in a single device (Boden, Figure 1; col. 3, line 51, to col. 4, line 1). Accordingly, one of ordinary skill in the art, in view of the disclosure of Ludovici and Boden, would have understood that IKE server 451 and IPSEC 452 are deployed on a single VPN device.

Applicants respectfully disagree with the Office's assertions that Ludovici discloses that "one of ordinary skill in the art would reasonably ascertain that the IPSEC and IKE server may be separate, as their communication goes through a separate server." Further, Applicants respectfully disagree with the Office's

assertions that Ludovici discloses that "since the correspondence between the VPNCNM and the IKE Server are networked requests, the IPSEC and IKE Server (as depicted in figure 22) must also be only communicatively connected, since they transact via the VPNCNM."

Applicants respectfully submit that the Office fails to substantiate its prior assertions with support from the teachings of Ludovici or of general knowledge to one of ordinary skill in the art. Ludovici fails to disclose or suggest the VPNCNM being separate, i.e. deployed in separate devices, from the IPSEC 452 and IKE Server 451. Rather, as previously noted, the teachings of Ludovici demonstrate that one of ordinary skill in the art would have understood that the IPSEC 452 and the IKE Server 451 are deployed on a single VPN device.

Further to the teachings discussed above, Ludovici describes implementing the VPNCNM as a process or job using "Object-Oriented Modeling and Design," i.e. object-oriented programming (Ludovici, col. 3, lines 30-64). Ludovici repeatedly refers to key management, encryption, authentication, security policy, and server as objects of "Object-Oriented Modeling and Design" (Ludovici, Figs. 9A, 9B, 15-18, and 20, and the corresponding descriptions of the disclosure). Hence, the VPNCNM is a software object, rather than a physical device.

Furthermore, Ludovici discloses that an objective of his invention is to provide *central* management of connections (Ludovici, col. 3, lines 18-22). Hence, an objective of his invention is to centralize connection management components, rather than

distributing the components. Accordingly, the teachings of Ludovici combined with the general knowledge of one of ordinary skill in the art for VPNCNM would have led to an understanding that the VPNCNM software process would have been implemented on a single device together with the IPSEC 452 and IKE Server 451 to centralize the components of the system, particularly because it is well known in the art that both the IPSEC 452 and IKE Server 451 are also typically implemented as software processes, i.e. as an IPSEC protocol stack and an IKE daemon, respectively.

Furthermore, Applicants respectfully submit that the Office fails to substantiate its assertions that "since the correspondence between the VPNCNM and the IKE Server are networked requests, the IPSEC and IKE Server (as depicted in figure 22) must also be only communicatively connected, since they transact via the VPNCNM." Ludovici fails to disclose or suggest the requests between the VPNCNM and the IKE Server 451 being networked requests.

Rather, Ludovici discloses that the correspondence comprise StartP2SA, StopP2SA, StartedP2SA, StoppedP2SA, Response, and Load/Unload messages (Ludovici, col. 9, lines 14-21). Ludovici fails to disclose or suggest that the correspondence between the VPNCNM and the IKE Server are networked requests.

Accordingly, Applicants respectfully submit that the Office Action fails to establish a *prima facie* case of anticipation of the pending claims over the teachings of Ludovici.

Accordingly, the Office Action fails to demonstrate that Ludovici discloses or suggests every feature recited in claim 1, and similarly recited in claims 10 and 13.

Claims 2-6 and 8 depend from claim 1. Claims 11-12 depend from claim 10. Accordingly, claims 2-6, 8 and 11-12 should be allowable for at least their dependency upon an allowable base claim, and for the specific limitations recited therein.

Therefore, Applicants respectfully request withdrawal of the rejections of claims 1-6, 8, and 10-13 under 35 U.S.C. §102(e), and respectfully submit that claims 1, 10 and 13, and the claims that depend therefrom, are now in condition for allowance.

Claim Rejections under 35 U.S.C. §103(a)

The Office Action rejected claims 7 and 9 under 35 U.S.C. §103(a) as allegedly unpatentable as obvious over Ludovici.

Ludovici was discussed above. As previously noted, Ludovici fails to disclose or suggest every claim feature recited in claim 1. The Office took Official Notice that it is well known to use out-of-band LANs for management traffic for preventing interlopers from being able to monitor it. Applicants respectfully submit that the Office's taking Official Notice fails to cure the deficiencies of Ludovici discussed above with respect to the features recited in claim 1. Claims 7 and 9 depend from claim 1. Accordingly, claims 7 and 9 should be allowable for at least their dependency upon an allowable base claim, and for the limitations recited therein.

Therefore, Applicants respectfully request withdrawal of the rejection of claims 7 and 9 under 35 U.S.C. §103(a), and respectfully submit that claim 1, and the claims that depend therefrom are now in condition for allowance.

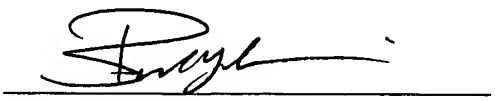
CONCLUSION

In conclusion, Applicants respectfully submit that Ludovici fails to disclose or suggest every claim feature recited in claims 1-20. The distinctions previously noted are more than sufficient to render the claimed invention unanticipated and non-obvious. It is therefore respectfully requested that all of claims 1-20 be allowed, and this present application be passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, Applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, Applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Brad Y. Chin
Registration No. 52,738

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

BYC:dlh

Enclosures: Additional Claim Fee Transmittal
Check No. 018174